

**UNITED STATES DISTRICT COURT  
DISTRICT OF MINNESOTA**

---

Jacqueline Mekhail, individually, and on  
behalf of those similarly situated,

No. 23-CV-00440 (KMM/TNL)

Plaintiff,

**ORDER**

v.

North Memorial Health Care, d/b/a North  
Memorial Health,

Defendant.

---

This matter is before the Court on Defendant North Memorial Health Care’s (“North”) motion to dismiss (ECF 29 (“Motion”)) Plaintiff Jacqueline Mekhail’s (“Ms. Mekhail”) First Amended Complaint (ECF 22 (“FAC”)). For the reasons set forth below, the Motion is **GRANTED IN PART** and **DENIED IN PART**.

**I. Background**

This case sits at the intersection of internet and medical privacy. Ms. Mekhail alleges that North’s use of a piece of hidden software on its websites surreptitiously tracked, collected, and monetized various aspects of her<sup>1</sup> online activity, including sensitive medical information protected by law. Ms. Mekhail filed her complaint on February 22, 2023. ECF

1. After North moved to dismiss the complaint (ECF 15), Ms. Mekhail amended her

---

<sup>1</sup> This lawsuit is also brought on behalf of a putative class, and the operative complaint includes class allegations relevant to individuals other than Ms. Mekhail. *See* ECF 22 at 41–45. The pending motion does not address these class allegations and class certification has not yet been sought.

complaint by right, and North's motion was withdrawn. The FAC added new factual allegations and claims. Ms. Mekhail now asserts seven causes of action: violations of the federal and Minnesota wiretap statutes (Counts I and II), the Minnesota consumer fraud statute (Count III), the Minnesota deceptive trade practices statute (Count IV), and the Minnesota health records statute (Count V); as well as common law claims of invasion of privacy and unjust enrichment (Counts XI and XII). *See* ECF 22 at 45–64. North then filed the pending Motion (ECF 29), once again asking the Court to dismiss each of Ms. Mekhail's claims, pursuant to Federal Rule 12(b)(6). *See* ECF 31 (North's Memorandum in Support of Motion to Dismiss) at 1. The parties submitted full briefing on the pending motion, and a hearing was held. Various supplemental filings were also submitted by the parties.

#### **A. Alleged Facts**

North is a Minnesota-based health care provider and Ms. Mekhail is a Minnesota resident and former North patient. The tracking software at issue is known as a "pixel" (hereinafter, the "Pixel") and was developed by the technology company Meta, formerly known as Facebook. Meta is not a party to this lawsuit. Ms. Mekhail's allegations concern two different websites (hereinafter, collectively, the "Websites"): first, North's public-facing website, [www.northmemorial.com](http://www.northmemorial.com), which publicly offers information about medical issues and the health care resources provided by North; second, North's password-protected "patient portal," which contains personal medical information, including patient

records, appointment booking, and test results, at <https://northmemorial.com/mychart-medical-records/>. Ms. Mekhail alleges that North embedded the Pixel into the source code of both Websites. *See* ECF 22 ¶ 5 (“Recently, Plaintiff became aware that Defendant incorporates Meta tracking technology, the Pixel, on the North Memorial Websites.”).

According to Ms. Mekhail’s allegation, the Websites were essential to her experience as a North patient. She states that North “encouraged and advised [her] to utilize Defendant’s online website and patient portal to make appointments, track and receive test results, receive medical treatment, communicate with medical professionals, including doctors, nurses, and other staff, and exchange private, personal, and in most cases confidential information regarding her treatment.” *Id.* ¶ 20. She further states that North provides policies (the “Privacy Policy”) that assure Website users that their medical privacy and health data will be protected. *See, e.g., id.* ¶¶ 107–108. In essence, each of Ms. Mekhail’s claims is rooted in the allegation that while she engaged with the Websites at North’s encouragement, the Pixel was surreptitiously tracking, collecting, and transmitting her online activity, including page views, clicks, search terms, and so forth. This information was then allegedly collated by Meta and eventually used to craft targeted advertising to Ms. Mekhail related to her web activity.

In short, because of the nature of the activity that was allegedly tracked and where it took place (i.e., on her health provider’s public- and private-facing Websites), Ms. Mekhail contends that the Pixel was able to access disclosed protected health information

without her consent, in violation of several laws. North, in turn, argues that Ms. Mekhail's allegations cannot legally support any of her claims and asks this Court to dismiss the FAC in its entirety. Having carefully considered the arguments and submissions of both parties, and for the reasons stated below, the Court grants North's motion as to Counts III and VI and denies it as to Counts I, II, IV, V, and VII.

## **II. Legal Standard**

To survive a Rule 12(b)(6) motion to dismiss, a complaint must contain "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). This standard does not require the inclusion of detailed factual allegations in a pleading, but the complaint must contain facts with enough specificity "to raise a right to relief above the speculative level." *Id.* at 555. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements," are not sufficient. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 555). In applying this standard, the Court must assume the facts in the complaint to be true and take all reasonable inferences from those facts in the light most favorable to the plaintiff. *Morton v. Becker*, 793 F.2d 185, 187 (8th Cir. 1986); *see also Waters v. Madson*, 921 F.3d 725, 734 (8th Cir. 2019).

### III. Analysis

#### A. Wiretap Statutes (Counts I and II)

Ms. Mekhail brings claims under the federal Electronic Communications Privacy Act (“ECPA”) and the Minnesota Protection of Communications Act (“MPCA”). These statutes are “nearly identical” and, therefore, analyzed together by courts in this District. *Wilson v. McRae’s US Mail Serv. Inc.*, No. 20-01664, 2020 WL 6808861, at \*4 (D. Minn. Oct. 29, 2020), *report and recommendation adopted*, No. 020CV01664PJSKMM, 2020 WL 6802395 (D. Minn. Nov. 19, 2020) (internal quotation marks omitted). As such, Ms. Mekhail’s allegations under both wiretap statutes rise or fall together.

The ECPA and the MPCA prohibit the unauthorized interception of electronic communications. *See generally* 18 U.S.C. § 2511(1); Minn. Stat. § 626A.02. Both statutes provide a civil remedy for those whose communications are unlawfully intercepted. *Id.* at § 2520; Minn.Stat. 626A.02, subd. 5. “A plaintiff pleads a prima facie case under [EPCA] by showing that the defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device. *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 135 (3d Cir. 2015) (quoting *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 18 (1st Cir. 2003)). It is also a violation of the ECPA to use the contents of a communication that a person knows was unlawfully intercepted. 18 U.S.C. §

2511(1)(d); *see also Bartnicki v. Vopper*, 532 U.S. 514, 529 (2001) (discussing the “use” provision of § 2511(1)(d) as distinct from the act of intercepting under § 2511(1)(a)).

North argues that Ms. Mekhail has failed to plead the interception of contents within the meaning of the statute. ECF 31 at 8–9. North also argues that the so-called “party exception” applies to the conduct alleged in the FAC, and therefore, the ECPA claims must be dismissed. *Id.* at 7–10. The Court disagrees, but before explaining its decision, it must clarify how it interprets certain mechanics of Ms. Mekhail’s allegations.

In the FAC, Ms. Mekhail asserts that North is liable for making interceptions, the procurement of Meta to intercept, and the use of interceptions made by Meta. The factual bases for these contentions are somewhat in tension with each other. At times, Ms. Mekhail contends that North intercepted and then sent data to Meta. *See, e.g.*, ECF 22 ¶ 37 (“Every time *Defendant sends* patients’ data to Meta, the patients’ Sensitive Information is unlawfully disclosed.”) (emphasis added); *id.* ¶ 72 (“Defendant’s source code manipulates website visitor’s browsers by secretly instructing it to duplicate the Website Communications and *sending those communications to* Meta.”) (emphasis added). At other times, the FAC alleges that Meta, via the Pixel, did the interception. *See, e.g., id.* ¶ 31 (describing a “privacy violation . . . in which *Defendant intentionally granted access to third-party Meta to record and collect* information on the company’s systems. . . .”) (emphasis added); *id.* ¶ 35 (“Because Defendant utilizes Meta’s Pixel, *Meta’s code surreptitiously duplicates* the communication from the user to Defendant *and sends it to*

*Meta's own servers*, along with additional information that includes the user's identity.”) (emphasis added); *id.* ¶ 49 (“Through [the Pixel], *Meta intercepts* each page a user visits, what buttons they click, as well as specific information they input into the website and what they searched. *Pixel sends each of these pieces of information to Meta.* . . .”) (emphasis added).

An interceptor and the procurer/user of an interception are conceptually and legally distinct. *See Reynolds v. Spears*, 93 F.3d 428, 432 (8th Cir. 1996) (concluding that a first person's “listening to telephone conversations that [a second person] had unlawfully recorded are not interceptions” by the first person). And since it does not appear that, factually, the FAC is describing different categories of interceptions, the Court is skeptical that North and Meta can both be the perpetrators of the same interceptions under the terms of Ms. Mekhail's own allegations. However, the Court's concern about this nuance was rendered moot because, during the hearing on the pending motion, counsel for Ms. Mekhail explicitly disavowed the theory that North had acted as an interceptor, explaining that she would proceed on the theory that North had procured and/or used Meta's interceptions. *See* ECF 48 (Mot. to D. Hr'ng Tr.) at 56:4-18. The extent to which this apparent narrowing matters is discussed in further detail below.

### ***Prima Facie Case***

North contends that Ms. Mekhail has failed to plead the interception of contents within the meaning of the statute. ECF 31 at 8–9. The Court disagrees.

“Intercept” is defined under the Wiretap Act as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). Here, Ms. Mekhail has alleged that North procured Meta to embed the Pixel within the source code of North’s Websites, and likewise has plausibly alleged that an interception occurred. For example, Ms. Mekhail alleges that “Defendant utilizes Meta’s Pixel, [and] Meta’s code surreptitiously duplicates the communication from the user to Defendant and sends it to Meta’s own servers, along with additional information that includes the user’s identity.” ECF 22 at 10–11. This is a straightforward allegation, plausible in light of the broader allegations of the FAC. Ms. Mekhail has sufficiently pleaded an interception.

“Contents” are defined as “any information concerning the substance, purport, or meaning of [a] communication.” 18 U.S.C. § 2510(8). One of the central disagreements in this case is whether search queries and other data that suggest, but do not outright state, information about Ms. Mekhail’s health and patient status are substantive “contents” or merely “record information” that is characteristic of the substantive communication. *See, e.g.*, ECF 31 at 8. North relies upon a Ninth Circuit case to argue that “information such as names, Facebook IDs, and webpage addresses [does] not constitute ‘contents’ under the ECPA.” *Id.* at 8 (citing *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106–08 (9th Cir. 2014)). *Zynga* is not binding on this Court and, in any event, held out the possibility that narrative search queries revealed via URLs could represent “contents” under certain circumstances.



*See* 750 F.3d at 1108–09 (“Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication.”). And Ms. Mekhail’s FAC alleges exactly that kind of revelation of substantive health information via the interception of narratives contained within URLs. *See, e.g.*, ECF 22 at 21–24. But the Court need not decide at this juncture whether URLs, webpage addresses, and the like constitute “contents” because Ms. Mekhail’s FAC goes much farther, clearly alleging that substantive information, including details about medical appointments, conditions, and treatments, was obtained via the Pixel. *See, e.g.*, ECF 22 at 4, 7, 11. Specifically, the FAC claims that the Pixel was in place and collecting information on both of North’s Websites: the public-facing one and the patient portal. To be sure, North hotly disputes that this kind of information was revealed, but the Court does not adjudicate factual disputes on a motion to dismiss. Ms. Mekhail has sufficiently pleaded that “contents” were intercepted.

### ***The Party Exception***

The ECPA provides an exception to liability when the person intercepting a communication is also a “party to the communication.” 18 U.S.C. § 2511(2)(d). This is referred to as the “party exception.” North argues that the party exception applies to the alleged conduct in the FAC, and therefore, the ECPA claims must be dismissed. ECF 31 at 7–10.

As the FAC makes clear, the Pixel is alleged to have taken Ms. Mekhail's data during the passing of digital information between Ms. Mekhail and North while Ms. Mekhail was using North's Websites. As such, North is a party to the relevant communications. *See In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 143 (3d Cir. 2015) ("[T]he intended recipient of a communication is necessarily one of its parties").

Ms. Mekhail argues that only a direct interceptor can invoke the party exception, and that no party exception applies in procurement and use scenarios. ECF 37 at 11, 26. Indeed, the statute's plain language appears to support the interpretation that the party exception was drafted with active interceptors foremost in mind. *See* § 2511(2)(d) ("It shall not be unlawful under this chapter for a person not acting under color of law *to intercept* a wire, oral, or electronic communication where such person is a party to the communication.") (emphasis added). However, whether this means the statute excludes party procurers and users of others' interceptions from the party exception is less clear. Judge Blackwell, in a similar case to this one, recently noted that "[t]he Eighth Circuit has not addressed the question of whether an intended recipient party to a communication [can invoke the party defense] when there is simultaneous duplication and forwarding of information *to* a third party." *In re Grp. Health Plan Litig.*, No. 23-CV-267 (JWB/DJF), 2023 WL 8850243, at \*7 (D. Minn. Dec. 21, 2023) (ultimately applying the party exception to the alleged conduct in that case) (emphasis added). This analysis does not speak directly

to the scenario presented here, which is whether the exception can be invoked where a party to a communication has allegedly procured another to intercept the same communication they were a party to or has used a third parties' interception of the same communication. No circuit, nor any court, appears to have addressed a similar fact pattern in the context of the party exception.

Here, the Court will assume without deciding that the party exception presumptively applies to *any* alleged violation of ECPA, whether a party to a communication is accused of directly intercepting that communication or whether they are accused of procuring/using an interception of that communication. The Court's assumption is informed by several factors. First, the assumption is generally consistent with persuasive ECPA case law concerning the "presumptive non-liability of parties." *See id.* (citing *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d at 144). Second, although counsel represented at the hearing that North is no longer alleged to be an active interceptor, the operative complaint stated otherwise. Therefore much of the briefing on this issue was directed toward the more straightforward legal question of whether North, as an alleged interceptor, can deploy the party exception and win dismissal of the FAC. Consequently, arguments specific to whether the party exception applies to a procurer/user of another's

interception are undeveloped.<sup>2</sup> Most importantly, the Court’s decision to apply the party exception in this Order does not change the outcome because the Court concludes that Ms. Mekhail has adequately pleaded a criminal or tortious act, sufficient to invoke the “crime-tort exception” to the party exception.

The crime-tort exception-to-the-exception applies if a party intercepts a communication “for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C. § 2511(2)(d). Its contours are somewhat unclear. Several circuits have determined that, to plead the crime-tort exception, the allegedly unlawful act must be independent of the allegedly unlawful interception. *See, e.g., Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010); *Sussman v. American Broadcasting Cos.*, 186 F.3d 1200, 1201–03 (9th Cir.1999). Other courts find that the crime-tort exception applies only where either the “primary motivation” or

---

<sup>2</sup> The Court’s assumption is not a ruling, and nothing prevents Ms. Mekhail from renewing her arguments around limitations to the party exception later in this litigation, should the facts necessitate. And given Ms. Mekhail’s clarification regarding her theory that North did not act as an interceptor, the Court would expect more focused and germane briefing on the issue if it is raised again.

“determinative factor” in a party’s interception was to commit a crime or tort.<sup>3</sup> *See United States v. Dale*, 991 F.2d 819, 842 (D.C. Cir. 1993); *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778 (N.D. Cal. 2022); *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 514–15 (S.D.N.Y. 2001); *cf Caro*, 618 F.3d 94 (2d Cir. 2010) (eschewing a hierarchy of intent and observing merely that “if, at the time of the recording, the offender plans to use the recording to harm the other party to the conversation, a civil cause of action exists. . . .”).

---

<sup>3</sup> The “primary motivation” or “determinative factor” test does not appear in the statute, which inquires only about a criminal or tortious “purpose” behind an interception. *See* 18 U.S.C. § 2511(2)(d). Nor does the test appear in any authority binding on this Court. Instead, it seems that the test originated in a 1986 case from the District of Massachusetts, which extrapolates from Eighth Circuit dicta and other sources to conclude that § 2511(2)(d) requires more than its plain language says it does. *See United States v. Vest*, 639 F. Supp. 899 (D. Mass. 1986) (citing, *inter alia*, *United States v. Phillips*, 564 F.2d 32, 34 (8th Cir. 1977)).

Here, Ms. Mekhail alleges that the interceptions were made to access and monetize<sup>4</sup> her private and protected health data. As the Court explains below, the allegation that the Pixel allowed Meta to access Ms. Mekhail’s private health data, with the purpose of monetizing that data, is sufficient to plead a violation of Minnesota health records law and state a claim for unjust enrichment. Further, Ms. Mekhail’s complaint also invokes, albeit does not claim direct liability under, the federal Health Insurance Portability and Accountability Act, commonly known as HIPAA, the alleged violation of which has recently been found sufficient to invoke the crime-tort exception. *See Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2023 WL 8544084, at \*3 (N.D. Ill. Dec. 11, 2023) (plaintiff plausibly stated an ECPA claim and invoked the crime-tort exception by alleging violations of HIPAA arising out of the alleged interception). As such, Ms. Mekhail’s allegations sufficiently plead an interception made with the purpose of violating one or more laws, independent from the act of interception itself. Of course, the parties require discovery to

---

<sup>4</sup> North cites case law from different districts for the proposition that the crime-tort exception is inapplicable where a defendant’s motivation is pecuniary. *See* ECF 31 at 9–10. The Court is aware that the Northern District of California appears to have adopted this approach. *See, e.g., In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 797 (N.D. Cal. 2022) (discussing various holdings from the Northern District of California that the tort exception does not exist where an alleged tortfeasor’s “motivation was to make money, not to injure plaintiff’s tortiously”). The Court will not follow such a bright-line rule in deciding the pending motion. Setting aside that a nuanced and factual differentiation of intent is improper at the pleading stage, the Court has serious doubts that a pecuniary purpose and an injurious purpose can always be so clearly distinguished. And it defies common sense that a clearly harmful act could escape liability as long as it was done for profit. Ultimately, the scope of conduct implicated by § 2511(2)(d) “must be determined on a case-by-case basis.” *Meredith v. Gavin*, 446 F.2d 794, 799 (8th Cir. 1971).

determine whether North's actions do, in fact, constitute conduct required to invoke the crime-tort exception. But at this stage, Ms. Mekhail's ECPA and MCPA claims may proceed. *See In re Grp. Health Plan Litig.*, 2023 WL 8850243, at \*8 ("While Plaintiffs have alleged HealthPartners' motivations, determination of HealthPartners' *actual* purpose for installing and using the Pixel Code requires a factual undertaking.").

North's motion is therefore denied as to Counts I and II.

**B. Minnesota Consumer Fraud Act (Count III)**

The MCFA prohibits the "act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise." Minn. Stat. § 325.69, subd. 1. North moves to dismiss Ms. Mekhail's MCFA claims for 1) a failure to plead fraud with particularity under Federal Rule of Civil Procedure 9(b); 2) a failure to plead intent; 3) a failure to plead a public benefit sufficient to invoke the MCFA's private attorney general provision; 4) a failure to allege a misrepresentation in connection with "merchandise;" and 5) a lack of causal nexus between alleged wrongful conduct and alleged harms. The Court need not address all these arguments because it agrees that Ms. Mekhail has failed to allege a misrepresentation in connection with merchandise, as required by the statute.

The MCFA "does not apply to all allegations of fraud, but only to those where there is a nexus between the alleged fraud and the sale of merchandise." *Grady v.*

*Progressive Direct Ins. Co.*, 643 F. Supp. 3d 929, 935 (D. Minn. 2022) (quoting *Banbury v. Omnitrition Int’l, Inc.*, 533 N.W.2d 876, 882 (Minn. Ct. App. 1995)); *see also Moua v. Jani-King of Minnesota, Inc.*, 613 F. Supp. 2d 1103, 1113 (D. Minn. 2009) (dismissing an MCFA claim where the alleged misrepresentations were unrelated to the sale of merchandise). The statute defines merchandise as “any objects, wares, goods, commodities, intangibles, real estate, loans, or services.” Minn. Stat. § 325F.68, Subd. 2. North argues that there is a lack of connection between the misrepresentations alleged by Ms. Mekhail—namely, North’s statement that it “protect[s] health and medical information as required by federal and state privacy law,” when, in fact, the Pixel allegedly violated such laws (*see, e.g.*, ECF 37 at 30)—and the sale of any merchandise. *See* ECF 31 at 18. Ms. Mekhail did not address this argument in her opposition to the pending motion, but at the hearing, counsel offered the theory that the “exchange of data” between Ms. Mekhail and North represented an intangible good or commodity, and otherwise deferred to the content of the FAC to substantiate the merchandise requirement of this claim.

The problem for Ms. Mekhail is that the FAC does not actually point to the exchange of data between Ms. Mekhail and North as the relevant “merchandise.” What the FAC alleges is that “[t]he medical services that Defendant markets, provides, offers, and/or sells are considered merchandise” under the statutory definition. *See* ECF 22 ¶ 170. The statutory definition of “merchandise” includes “services,” and the Court



assumes that “medical services” would, therefore, qualify as services. But Ms. Mekhail is not alleging that there was a misrepresentation made by North in connection with its provision of any medical services. Ms. Mekhail alleges that when she visited the North Websites, her private data was taken by the Pixel in violation of state or federal law and in contradiction to North’s statements that it would protect her privacy. This alleges a misrepresentation related to data privacy, but North is not in the business of providing data privacy services. Therefore, the Court concludes that Ms. Mekhail has failed to adequately allege a nexus between the stated misrepresentation by North and the “sale of any merchandise” by North. *See Moua*, 613 F. Supp. 2d at 1113 (dismissing MCFA claim and explaining that “[t]he critical issue is not . . . whether [an allegedly fraudulent] sale involved aspects that can be viewed as constituting ‘merchandise,’ but rather whether there is a ‘nexus’ between the alleged misrepresentations and that ‘merchandise’”).

North’s motion is therefore granted as to Count III.

### **C. Minnesota Uniform Deceptive Trade Practices Act (Count IV)**

The Minnesota Unfair and Deceptive Trade Practices Act (“MUDTPA”) prohibits the use of “deceptive trade practices” in the course of business, vocation, or occupation. Minn. Stat. § 325D.44. Such deceptive practices include “caus[ing] likelihood of confusion or of misunderstanding as to . . . certification of goods or services,” “engag[ing] in (i) unfair methods of competition, or (ii) unfair or unconscionable acts or practices,” and “engag[ing] in any other conduct which similarly creates a likelihood of

confusion or misunderstanding.” *Id.* at subd. 1(2), (13), (14).

North moves to dismiss Ms. Mekhail’s MUDPTA claims for three reasons: first, that she has failed to plead them with particularity as required by Rule 9(b); second, she has failed to plead facts establishing her entitlement to the injunctive relief offered by the statute; and third, she lacks Article III standing to bring her claim for injunctive relief. The second and third bases involve essentially the same legal questions and will be analyzed together. For the following reasons, North’s motion is denied with respect to Count IV.

### ***Particularity***

Rule 9(b) requires that “[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake.” Fed. Rule. Civ. P. 9(b). The Rule 9(b) standard applies to MUDPTA. *E-Shops Corp. v. U.S. Bank Nat. Ass’n*, 678 F.3d 659, 665 (8th Cir. 2012). This means that to state a claim under MUDPTA, the complaint must set forth “the who, what, when, where, and how” of the alleged violation of the act. *Id.* at 666. However, where plaintiff’s theory is one of fraudulent omission, rather than active misrepresentation, Rule 9(b) may be “satisfied if the omitted information is identified and ‘how or when’ the concealment occurred.” *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1311 (D. Minn. 2014) (internal citations omitted). The main purpose of Rule 9(b) is to create notice. *Commercial Prop. Invs., Inc. v. Quality Inns Int’l, Inc.*, 61 F.3d 639, 644 (8th Cir. 1995)

(describing the purpose as to “facilitate a defendant's ability to respond and to prepare a defense to charges of fraud”). Therefore, the level of particularity required varies along with the facts of each case. *BJC Health Sys. v. Columbia Cas. Co.*, 478 F.3d 908, 917 (8th Cir. 2007).

Here, Ms. Mekhail’s FAC alleges both misrepresentations and omissions relevant to its MUDPTA claim. *See* ECF 22 ¶ 179. However, North argues that in opposing the pending motion, Ms. Mekhail has effectively abandoned a misrepresentation theory and now advances only a fraudulent omission theory. ECF 39 at 16 (“Plaintiff appears to have abandoned any misrepresentation theory”). Admittedly, Ms. Mekhail’s briefing is somewhat scattered on whether North is alleged to have made active misrepresentations or misrepresentations by omission, but the operative complaint clearly alleges both (ECF 22 ¶ 179). Further, Ms. Mekhail’s briefing does ultimately address the full “who, what, when, where, and how” requirement under *E-Shops* (for misrepresentations) rather than merely the “how and when” required under *In re Target Corp* (for omissions). *See* ECF 37 at 50–51. Accordingly, the Court concludes that Ms. Mekhail intends to proceed under both theories and assesses the adequacy of the FAC as to all five particularity elements.

First, the Court finds that “who,” “when,” and “where” are sufficiently pleaded, as identified in Ms. Mekhail’s brief. *See id.* (identifying “who” as North; “when” as October 2021 to the present day; and “where” as North’s Websites and the state of Minnesota). None of these elements appear to be in dispute and none require further

elaboration or analysis. As for “what” the Court concludes the element is satisfied by the allegation that North made numerous statements that it protected patients’ medical privacy and health data. *See, e.g.*, ECF 22 ¶ 4 (alleging that “Defendant represents to patients that its online patient portal is both a secure platform, and the information provided therein will remain secure and confidential”); ¶ 28 (alleging that North states that “North Memorial Health is committed to ensuring that your privacy is protected”); ¶ 108 (alleging that North states that “[w]e protect health and medical information as required by federal and state privacy laws” and that “North Memorial is committed to ensuring that your privacy is protected”); ¶¶ 109–110 (alleging that North makes statements about its tracking cookies designed to create confidence about data security and privacy). Finally, as for “how” these statements are deceptive, this is satisfied by the numerous allegations that North did not, in fact, protect Ms. Mekhail’s and other patients’ medical privacy and health data, because it shared private health data with Meta without Ms. Mekhail’s consent or awareness. *See, e.g., id.* ¶¶ 4, 9, 11, 22, 23, 38, 40, 47, 72, 74, 116.

To be sure, North strongly disputes that the statements alleged by Ms. Mekhail actually constitute misrepresentations, in part because North thematically disputes that anything shared with Meta was protected health data and also because some of allegedly deceptive statements are linked to the Privacy Policy, which also (allegedly) states that North “may disclose information to third parties who act for us or on our behalf.” *Id.* ¶

108. But North overestimates both the extent to which this Court can engage in fact finding at the pleading stage and whether statements in the Privacy Policy can require dismissal at this stage in the litigation. North is essentially asking the Court to make factual determinations about the effect that the Privacy Policy had (or ought to have had) on Ms. Mekhail, weighing their interpretation of its meaning and import against hers. The Court's role at this stage is not to predict whether Ms. Mekhail will ultimately succeed at proving her claims of misrepresentations or actionable omissions. Instead, the Court must accept all facts alleged by Ms. Mekhail and draw all reasonable inferences in her favor. Consequently, the Court finds that the FAC complies with the particularity requirements of Rule 9(b). Accord *In re Grp. Health Plan Litig.*, 2023 WL 8850243, at \*8 (MUDPTA allegations met the requirements of Rule 9(b) where they were "sufficient to allow [defendant] to understand what is alleged and respond"); *In re Target Corp.*, 64 F. Supp. 3d at 1311 ("Although [plaintiffs'] allegations are not as detailed as [defendant] would like, at this early stage of the litigation . . . [p]laintiffs have complied with 9(b)."); *McGregor v. Uponor, Inc.*, No. CIV 09-1136 ADM/JJK, 2010 WL 55985, at \*4 (D. Minn. Jan. 4, 2010) ("Rule 9(b) does not require that a "complaint be suffused with every minute detail of a misrepresentation.") (internal quotations omitted);

### ***Injunctive Relief***

With respect to this portion of the FAC alone, Defendants' arguments regarding Article III standing present a challenge to the Court's subject matter jurisdiction pursuant

to Federal Rule of Civil Procedure 12(b)(1). Defendants raise a “facial” standing challenge, which is directed only to the pleadings and essentially applies the Rule 12(b)(6) standard. *See Osborn v. United States*, 918 F.2d 724, 729 n.6 (8th Cir. 1990). When considering a facial attack on jurisdiction, courts presume the facts alleged in the complaint to be true. *Titus v. Sullivan*, 4 F.3d 590, 593 (8th Cir. 1993).

For Ms. Mekhail<sup>5</sup> to meet the burden to allege Article III standing, she must show (1) an injury in fact that (2) is fairly traceable to the defendant's alleged conduct and (3) is likely to be redressed by a favorable court ruling. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). When a plaintiff seeks injunctive relief, “the ‘injury in fact’ element of standing requires a showing that the plaintiff faces a threat of ongoing or future harm.” *Park v. Forest Serv. of U.S.*, 205 F.3d 1034, 1037 (8th Cir. 2000); *see also City of Los Angeles v. Lyons*, 461 U.S. 95, 101–05, 107 n.8 (1983) (stating that the threat of future injury must be “real and immediate”).

A plaintiff “must demonstrate standing for each claim that they press and for each form of relief that they seek.” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021). MUDTPA provides an injunctive remedy. Minn. Stat. § 325D.45; *see also Barclay v.*

---

<sup>5</sup> As the named plaintiff in a putative class action, Ms. Mekhail must allege facts establishing the elements of her own standing, and may not rely on the injuries of unidentified class members. *Spokeo*, 578 U.S. at 338 & n.6; *see also In re SuperValu, Inc.*, 870 F.3d 763, 768 (8th Cir. 2017) (same).

*Icon Health & Fitness, Inc.*, No. 19-2970, 2022 WL 486999, at \*1 (D. Minn. Feb. 17, 2022) (“The M[U]DTPA’s only remedy is injunctive relief.”). The statute provides this remedy only for a “person likely to be damaged by a deceptive trade practice.” Minn. Stat. § 325D.45, subd. 1. Because MUDTPA provides injunctive relief only “for a person likely to be damaged,” it provides relief from future damage, not past damage.” *Lofquist v. Whitaker Buick-Jeep-Eagle, Inc.*, C5-01-767, 2001 WL 1530907 at \*2 (Minn. Ct. App. Dec. 4, 2001) (internal quotations omitted). As such, a MUDPTA claim requires a showing of likely future harm that is seemingly “indistinguishable from Article III’s threat-of-future-harm requirement for injunctive relief.” *Barclay*, 2022 WL 486999, at \*2 (D. Minn. Feb. 17, 2022) (“In other words, under the M[U]DTPA, like Article III, a plaintiff cannot obtain an injunction without showing a likelihood of future injury.”). Therefore, “to state a [MU]DTPA claim, the plaintiff must allege ‘a likelihood of future harm.’” *Jaskulske v. State Farm Mut. Auto. Ins. Co.*, No. 14-CV-869 PAM/TNL, 2014 WL 5530758, at \*6 (D. Minn. Nov. 3, 2014) (quoting *Gardner v. First Am. Title Ins. Co.*, 296 F.Supp.2d 1011, 1020 (D. Minn. 2003); *see also Knotts v. Nissan N. Am., Inc.*, 346 F. Supp. 3d 1310, 1328 (D. Minn. 2018) (“A plaintiff asserting a claim under the MDTPA must allege an irreparable injury or threat of future harm in order to withstand a motion to dismiss.”); *Cleveland v. Whirlpool Corp.*, 550 F. Supp. 3d 660 (D. Minn. 2021) (same).

Here, Ms. Mekhail argues that her pleadings allege a likelihood of future harm in two ways: where new data is taken from her by the Pixel, and where the data already

taken by the Pixel is used in newly harmful ways. ECF 37 at 39–40. The first scenario, in which Ms. Mekhail’s data is once again taken by the Pixel, is in obvious tension with the fact that Ms. Mekhail, by her own allegation, is a “former patient” of North. ECF 22 ¶ 19. Nevertheless, Ms. Mekhail argues that she may become a patient again, perhaps through an emergent scenario in which she cannot control the place of her treatment. ECF 37 at 40 (“It is unknown whether Plaintiff and the Class may be required to use North’s services, even if they may currently be former patients (for example, if taken to the emergency room and need follow up care.).”). In such a case, Ms. Mekhail argues that “she would be encouraged to use [North’s] Websites” once more. *Id.* This argument is essentially mirrored in the FAC at ¶¶ 187–88.

This first avenue of future harm is somewhat tenuous. By Ms. Mekhail’s allegation, *if* she is forced to avail herself of North’s medical services, then she would be *encouraged* to use the Websites and thereupon may be harmed again. This contingent scenario stretches the limits of a “real and immediate” threat required under *Lyons* and has led to dismissal in other deceptive trade practices cases. *See Johnson v. Bobcat Co.*, 175 F. Supp. 3d 1130, 1141 (D. Minn. 2016) (dismissing MUDPTA claims for lack of standing where plaintiff alleged that defendant’s “unlawful conduct is continuing” but failed to allege that the plaintiff “*intends* to purchase another” of defendant’s front-loader vehicles) (emphasis added). Allegations of deceptive trade practices that successfully articulate a likelihood of future harm to the original customer often feature special



circumstances that imply an ongoing relationship between the consumer and the defendant. *See, e.g., Cleveland*, 550 F. Supp. 3d at 677 (finding an adequate allegation of future harm where the plaintiff was a customer of an allegedly defective kitchen appliance who remained in an ongoing service relationship with the defendant and where the plaintiff alleged that any repair or replacement provided by the defendant would continue to suffer from the same, alleged defect). Still, and although it can be easy to forget in our society, the relationship of the patient to her medical provider is not merely one of the consumer to the free market. Unlike the purchaser of construction equipment or appliances, there are real and undeniable scenarios in which Ms. Mekhail, despite her best efforts, becomes a patient again<sup>6</sup> of North. And it is not clear to the Court that Ms. Mekhail could ever truly quantify the likelihood of such a scenario. After all, a medical emergency, like that contemplated in the pleadings, can arise as real and immediately as tomorrow or, with any luck, may never occur. It is simply not within Ms. Mekhail's capacity to plead the kind of concrete likelihood typically required by our standing cases.

Ms. Mekhail's second avenue for future harm is stronger. Here, her data, already collected by the Pixel, remains beyond her control and may be used in harmful ways.

---

<sup>6</sup> The Court also notes that because Ms. Mekhail was once a patient of North and she alleges that North has records of past treatment and appointments, she may have to use the patient portal even if she does not return as a patient. If she needs to obtain or review her own medical records from North using the portal (surely the quickest and least burdensome way) she would once again be exposed to harm from the allegedly deceptive practices.

ECF 37 at 40 (“Sensitive Information North previously collected and gathered in the past still exposes Plaintiff and the Class Members to a material risk of future harm that is concrete and imminent.”). This gets at a more tangible and immediate threat, and is one to which North has essentially no response. Admittedly, the threat contemplated by this scenario is only tangentially and ambiguously pleaded. *See, e.g.*, ECF 22 ¶¶ 13, 186, 206 (allegations that Ms. Mekhail continues to suffer harm from past disclosures of her data). But taking all allegations as true and viewing all inferences in Ms. Mekhail’s favor, it is enough.

Of course, the fact that Ms. Mekhail alleges a sufficient likelihood of future harm around the renewed collection and use of her data does not exactly mean that she is alleging that she is *likely to be deceived* by North again. Indeed, it seems unlikely that she would be. Courts grappling with this once bitten, twice shy conundrum in the standing context sometimes note that the threat of future harm can be situated in an injury other than a repeat case of deception. *See Davidson v. Kimberly-Clark Corp.*, 889 F.3d 956, 969 (9th Cir. 2018) (holding that a “previously deceived consumer” had standing to seek an injunction because of “the consumer’s plausible allegations that she will be unable to rely on the product’s advertising or labeling in the future, and so will not purchase the product although she would like to.”); *In re Gen. Mills Glyphosate Litig.*, No. CV 16-2869 (MJD/BRT), 2017 WL 2983877, at \*4 (D. Minn. July 12, 2017) (plaintiffs already allegedly deceived by a product label, still faced a threat of future

injury because they wished to continue purchasing the product, but absent an injunction, would “have no way of knowing in the future if the labels are accurate.”). And other courts recognize, requiring an individual who has already been deceived by a business practice to establish that they are likely to be deceived again by that practice defangs all aspects of public interest embodied in the deceptive trade statutes to the point of futility. *See Delgado v. Ocwen Loan Servicing, LLC*, 13-CV-4427, 2014 WL 4773991, at \*14 (E.D.N.Y. Sept. 24, 2014) (“Finding that Plaintiffs have no federal standing to enjoin a deceptive practice once they become aware of the scheme would eviscerate the intent of [legislatures] in creating consumer protection statutes.”); *Le v. Kohls Dep’t Stores, Inc.*, 160 F. Supp. 3d 1096, 1110 (E.D. Wis. 2016) (“[W]ere the Court to accept [the defendant’s] position that [the plaintiff’s] awareness of the alleged deception would operate to defeat standing for an injunction, then injunctive relief would never be available in false advertising cases, a wholly unrealistic result.”) (cleaned up).

The Court therefore concludes that Ms. Mekhail has pleaded an adequate likelihood of future harm to survive the pending motion. However, the Court observes that Ms. Mekhail will need to do more to actually obtain injunctive relief than she does to avoid dismissal on standing grounds. *See Barclay v. ICON Health & Fitness, Inc.*, No. 19-CV-2970 (ECT/DTS), 2020 WL 6083704 at \*5 n.2 (D. Minn. Oct. 15, 2020) (concluding that the argument that there is no threat of future injury once a plaintiff becomes aware of an allegedly deceptive practice is better suited for determining whether

the plaintiff is “entitled to injunctive relief on the merits, not whether they have standing”).

North’s motion is therefore denied as to Count IV.

**D. Minnesota Health Records Act (Count V)**

The MHRA prohibits healthcare providers from “release[ing] a patient’s health records to a person” without the patient’s consent or “specific authorization in law.” Minn. Stat. § 144.293, subd. 2. Under the MHRA, a “health record” includes “any information” that “relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient.” Minn. Stat. § 144.291, subd. 2(c). The MHRA “imposes liability on a person who negligently or intentionally releases a health record in violation of [the statute’s] guidelines.” *Rhoades v. Lourey*, No. A18-1120, 2019 WL 1006804, at \*2 (Minn. Ct. App. Mar. 4, 2019) (cleaned up) (citing Minn. Stat. §§ 144.293, subd. 1-2, .298, subd. 2(1)).

North argues that a “health record” under the MHRA does not extend to documents or records from which a person’s health condition or patient status can be “inferred” or “deduced.” ECF 31 at 26 (citing *Furlow v. Madonna Summit of Byron*, No. A19-0987, 2020 WL 413356, at \*2–3 (Minn. Ct. App. Jan. 27, 2020)). Instead, North argues that to qualify as a “health record,” a record must “expressly” state an individual’s past, present, or future physical or mental health condition as a patient or the provision

of health care. *Id.* (citing *Furlow*, 2020 WL 413356, at \*2). Consequently, North argues that Ms. Mekhail’s MHRA claim must be dismissed because her use of the North Websites amounts to “clicking around” to research medical issues, conditions, and providers, and any data collected by the Pixel could, therefore, “at most, permit an inference that Plaintiff, herself, might be experiencing a particular illness or looking for a particular doctor.” *Id.* at 27 (internal quotations omitted). The Court disagrees for several reasons.

### ***Inferential Information***

First, the Court disagrees that *Furlow* stands for such a bright-line proposition that documents or records that allow medical information to be inferred can never be “health records” within the meaning of the act. *Furlow* applied an earlier ruling, *Rhoades*, to conclude that a health record does not exist in an item from which “someone could merely deduce that someone is a patient of a facility.” *Furlow*, 2020 WL 413356, at \*3. The *Furlow* court consequently declined to find a “health record” in a photographic social media post because the post merely suggested where the plaintiff may have been a patient but revealed “nothing explicit[] . . . that goes to the nature of the [plaintiff’s] care or condition.” *Id.* Thus, *Furlow* is a limited holding that, like *Rhoades*, declines to expand the definition of a health record to include particular information creating inferences about whether or not a person *is* a patient or a provider.

Read appropriately, *Furlow* is inapt to the facts of this case. First, Ms. Mekhail

also alleges a specific operation of the Pixel, in which it would detect and disclose her attempts to log in to the password-protected patient portal. *See* ECF 22 ¶ 6 (“[W]hen [Ms. Mekhail] accessed the portal to sign in, the Pixel secretly deployed on the Websites sent the fact that she was attempting to login to the patient portal to Meta.”). Such operation of the Pixel implicates a disclosure of information that arguably reveals more than an inference of her status as a North patient and gets closer to outright revealing that she was a patient. This type of quasi-inferential, quasi-explicit disclosure is not addressed by the *Furlow* decision. Second, some of the inferences implicated in this case, which allegedly concern the provision of care and conditions, are broader than those in *Furlow*, which only addresses inferences about patient status. Indeed, the *Furlow* court appears to acknowledge this exact distinction by stating that the social media post was not a medical record *because* there was nothing in it that “goes to the nature of the care or condition” of the plaintiff. 2020 WL 413356, at \*3. Here, Ms. Mekhail is alleging that the data collected by the Pixel allowed Meta to glean details about her health condition, which was then exploited via targeted advertising. *See, e.g.*, ECF 23 ¶¶ 6, 9, 20, 23. Again, *Furlow* does not speak to these sorts of inferences.

### ***Explicit Information***

More critical than the adequacy of the inferences to be made from the public-facing website is the explicit health information gained from Pixel’s alleged presence on the private, patient-portal website. The Court finds that Ms. Mekhail alleges far more

than the kind of inferential data-collection that North prefers to address in the pending motion. As discussed above, Ms. Mekhail alleges that the Pixel operates on *both* Websites identified in the FAC. *See, e.g.*, ECF 22 at ¶ 5 (“Recently, Plaintiff became aware that Defendant incorporates Meta tracking technology, the Pixel, on the North Memorial Websites.”).

Here, Ms. Mekhail alleges that the patient portal allows patients to schedule appointments, attend remote e-visits with providers, communicate with providers, review medical test results, pay bills, arrange prescription refills, and more. ECF 22 at ¶ 3. Ms. Mekhail further alleges that the use of the Pixel on both Websites resulted in the alleged unauthorized disclosure of, among other things, appointments, including their type and procedures scheduled; information about patients’ providers; patient communications; patient insurance status; and patient gender and sexual orientation. *Id.* at ¶ 9. These allegations are sufficient to plead that health records within the meaning of the MHRA were released without Ms. Mekhail’s consent. *See In re Grp. Health Plan Litig.*, 2023 WL 8850243, at \*2 (finding that similar MHRA allegations were “sufficient to plausibly plead that health records were released . . . considering the broad definition of health records in the statute”).

North’s motion is therefore denied as to Count V.

### **E. Invasion of Privacy Claims (Count VI)**

The FAC asserts two distinct invasion of privacy torts in Count VI: publication of private facts and intrusion upon seclusion. ECF 22 at 61. A tortious publication of private facts occurs when someone “gives publicity to a matter concerning the private life of another if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.” *Bodah v. Lakeville Motor Express, Inc.*, 663 N.W.2d 550, 553 (Minn. 2003) (cleaned up). Intrusion upon seclusion occurs when someone “intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person.” *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 233 (Minn. 1998). North seeks to dismiss both. The Court agrees for the following reasons.

#### ***Publication of Private Facts***

Ms. Mekhail’s opposition brief to the pending motion did not respond to North’s arguments in favor of dismissal of the publication claim, and counsel for Ms. Mekhail confirmed at the hearing that she would abandon the claim due to a lack of factual basis to allege a sufficiently public dissemination of her health data. *See Bodah*, 663 N.W.2d at 557 (explaining that a publication of private facts requires that “the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.”).



### ***Intrusion Upon Seclusion***

Ms. Mekhail does contest North's arguments in favor of dismissing the intrusion claim. *See* ECF 37 at 46–49. However, counsel for Ms. Mekhail's clarification at the hearing that she was not alleging North to be an interceptor under the wiretap statute changes the landscape for the intrusion claim, as well. Courts have held that the act of intrusion is inseparable from the act of interception. *See Caro*, 618 F.3d at 101 (“Invasion of privacy through intrusion upon seclusion . . . is a tort that occurs through the act of interception itself.”). The Court agrees with this framing, and viewed in the inverse, an intrusion by North cannot be plausibly alleged where Ms. Mekhail concedes that it was Meta (or Meta's Pixel), rather than North, that made the interception. Since the factual allegations supporting the interception claims are the same as those supporting the intrusion claim, the Court concludes that North cannot be an alleged intruder if North is not the alleged interceptor.

North's motion as to Count VI is therefore granted.

### **F. Unjust Enrichment (Count VII)**

To state a claim for unjust enrichment, a plaintiff must allege facts showing “(1) a benefit conferred; (2) the defendant's appreciation and knowing acceptance of the benefit; and (3) the defendant's acceptance and retention of the benefit under such circumstances that it would be inequitable for him to retain it without paying for it.” *Christensen L. Off., PLLC v. Ngouambe*, No. A17-1917, 2018 WL 2293423, at \*6

(Minn. App. May 21, 2018). North argues that Ms. Mekhail’s unjust enrichment claim should be dismissed because she has failed to plead an implied contract between the parties and because Ms. Mekhail has not alleged any inequitable benefit received by North. The Court disagrees.

### ***Implied Contract***

Minnesota courts “limit[] the application of unjust enrichment to claims premised on an implied or quasi-contract between the claimant and the party alleged to be unjustly enriched.” *Caldas v. Affordable Granite & Stone, Inc.*, 820 N.W.2d 826, 838 (Minn. 2012). An implied contract “is an obligation raised or imposed by law and is independent of any real or expressed intent of the parties.” *Gaalswyk v. King*, No. CIV. 10-411 PJS/JSM, 2011 WL 4091858, at \*13 (D. Minn. Aug. 2, 2011), *report and recommendation adopted*, No. 10-CV-0411 PJS/JSM, 2011 WL 4095990 (D. Minn. Sept. 14, 2011) (quoting *Roske v. Ilykanyics*, 232 Minn. 383, 389, 45 N.W.2d 769, 774 (1951)). That being said, an implied contract “is in all respects a true contract. It requires a meeting of the minds the same as an express contract.” *Mjolsness v. Mjolsness*, 363 N.W.2d 839, 842 (Minn. Ct. App. 1985) (quoting *Balafas v. Balafas*, 117 N.W.2d 20, 25 (Minn. 1962)).

Ms. Mekhail alleges a reciprocal expectation that North would protect her medical data, implicitly pursuant to the requirements of state and federal law, such as HIPPA. *See, e.g.*, ECF 22 at 9, 33–37, 62. North, on the other hand, posits that this expectation

was in fact created by the Privacy Policy, which functioned as an express, rather than implied contract governing medical privacy. *See* ECF 31 at 35 n.13. And because Ms. Mekhail invokes this same policy in the FAC to substantiate certain of her other allegations (*see, e.g.*, ECF 22 ¶¶ 20, 28, 30, 107–18, 179), the document is fair game for consideration by the Court in deciding the pending motion. *See Porous Media Corp. v. Pall Corp.*, 186 F.3d 1077, 1079 (8th Cir. 1999) (Courts may consider “materials that are necessarily embraced by the pleadings” in considering a motion to dismiss under Rule 12(b)(6)). But, as previously explained above with respect to Ms. Mekhail’s MUDPTA claims, the Court will not adjudicate the effects and consequences of the Privacy Policy at this stage, and the mere fact of its existence is not incompatible with the legal sufficiency of Ms. Mekhail’s allegations.

Here, Ms. Mekhail has alleged that her expectation that North would protect her privacy flowed implicitly from well-known laws governing health privacy, rather than from the Privacy Policy. To the extent that North believes that any expectation was actually created by an explicit contract in the form of the Privacy Policy, such arguments are more appropriately considered with the benefit of a factual record, developed through discovery, and are not amenable to a legal determination at the pleading stage. *See Mjolsness*, 363 N.W.2d at 842 (“The question of whether there is [an implied contract] usually is to be determined by the trier of facts as an inference of fact to be drawn.”) (quoting *Balafas*, 117 N.W.2d at 25); *see also Gisairo v. Lenovo (United States) Inc.*, 516

F. Supp. 3d 880 (D. Minn. 2021) (explaining that unjust enrichment claims are routinely allowed to proceed in the alternative).

***Benefit to North***

North characterizes the FAC as “provid[ing] only a vague and conclusory allegation that Plaintiff conferred a benefit on North . . . without providing any details, including who allegedly provided the monetary compensation.” ECF 31 at 33. Ms. Mekhail states that North “knowingly and unlawfully received a benefit from its use of Plaintiff’s and the Class members’ Sensitive Information, including monetary compensation,” and that it would be “inequitable and unjust for Defendant to retain any of the profit or other financial benefits derived from the secret, unfair, and deceptive data tracking methods Defendant employees [sic].” ECF 22 ¶¶ 211, 213. Elsewhere, the FAC lays out assertions about the value of Ms. Mekhail’s data that was allegedly collected by the Pixel (ECF 22 at 26–30), as well as allegations about the ways that data was deployed to North’s benefit through its alleged use of the data in targeted advertisements (*see e.g., id.* at 7, 15). Taken together, these sections of the FAC sufficiently allege that a benefit was conferred on North by monetizing Ms. Mekhail’s data.

North also argues that the FAC fails to adequately allege that the benefit to North was inequitable in light of the previously discussed privacy policy. *See* ECF 31 at 33 (arguing that “Plaintiff’s use of the website cannot plausibly be inequitable” because she agreed to the terms of the privacy policy); *id.* at 35 (“It is not plausibly ‘unjust’ for North

to act consistently with [the privacy policy].”). But Ms. Mekhail does expressly plead that the collection was inequitable because it was uncompensated. And the Court again declines to explore the contours of the privacy policy at this stage. North may present its arguments concerning the equities of that policy with the benefit of a factual record developed in discovery.

North’s motion as to Count VII is therefore denied.

#### **IV. Order**

For the foregoing reasons, **IT IS HEREBY ORDERED that:**

1. Defendant’s Motion to Dismiss (ECF 29) is **GRANTED in part and DENIED in part;**
2. The Motion is **GRANTED** to the extent that Counts III and VI are **DISMISSED WITHOUT PREJUDICE**; and
3. The Motion is otherwise **DENIED**.

Date: March 28, 2024

*s/ Katherine M. Menendez*

Katherine M. Menendez  
United States District Judge